Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2015–2016

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

196

Vragen van het lid **Gesthuizen** (SP) aan de Minister van Veiligheid en Justitie over *het bericht dat het nieuwe tapbeleid van Justitie een aanval is op onze grondrechten* (ingezonden 10 september 2015)

Antwoord van Minister **van der Steur** (Veiligheid en Justitie) (ontvangen 5 oktober 2015)

Vraag 1 en 2
Wat is uw reactie op de berichten dat de politie standaard telefoon en internet tapt?[1]
Wat houdt de nieuwe interceptiestandaard in? Leidt deze nieuwe standaard er inderdaad toe dat de politie nu standaard alle telefoon- én internetgegevens tapt? Zo nee, waarom niet?

Antwoord 1 en 2
Onder het plaatsen van een tap wordt begrepen het conform artikel 126m van het Wetboek van Strafvordering opnemen van communicatie die plaatsvindt via een communicatiedienst. Hieronder vallen zowel telefoonnummers, IP-adressen als emailadressen. Een tap wordt geplaatst op bijvoorbeeld een computer, tablet of mobiele telefoon. Wanneer de rechter-commissaris toestemming verleent voor het plaatsen van een tap op een mobiele telefoon gaat het om alle communicatie die via een toestel verloopt, dus zowel spraak als data (internetverkeer). Dit was al zo voordat de interceptiestandaard werd aangepast en dit blijft zo.
De interceptiestandaard is het overdrachtsprotocol tussen de aanbieders en de politie om tapgegevens op uniforme wijze technisch over te dragen. De gewijzigde standaard heeft geen betrekking op het juridisch kader, maar alleen op de techniek en het technische proces ten aanzien van tappen. Uitsluitend de wijze van technische overdracht van de tap tussen de aanbieder en de politie en de wijze waarop in de statistieken vervolgens het aantal taps kan worden geteld, zijn gewijzigd.
De nieuwe standaard, die gebaseerd is op de Europese standaard, vervangt twee oude standaarden waarvan er één werd gebruikt ten behoeve van het tappen van spraak en de ander voor het tappen van internetverkeer. De nieuwe standaard sluit daardoor beter aan bij de huidige stand van techniek

[1] http://computerworld.nl/overheid/87947-nieuw-tapbeleid-justitie--aanval-op-onze-grondrechten & http://computerworld.nl/overheid/87209-politie-tapt-nu-standaard-telefoon-en-internet

ah-tk-20152016-196
ISSN 0921 - 7398
’s-Gravenhage 2015

en praktijk. Er is geen sprake van een situatie dat nu standaard alle telefoon- en internetgegevens worden getapt. Indien naast het opnemen van communicatie via de mobiele telefoon (inclusief internetdata) ook het opnemen van andere internetverbindingen dringend noodzakelijk is voor het strafrechtelijk onderzoek, wordt daarvoor een aparte aanvraag gedaan en wordt deze aanvraag opnieuw door de officier van justitie en de rechter-commissaris getoetst.

Vraag 3 en 4
Waarom is tot deze meer ingrijpende opsporingsmethode overgegaan? Wat is hiervan de wettelijke grondslag?
Acht u het proportioneel en legitiem om standaard over te gaan tot het tappen van zowel telefoon als internet? Zo ja, waarom?

Antwoord 3 en 4
Er is geen sprake van een meer ingrijpende opsporingsmethode. Het juridisch kader en de opsporingspraktijk ten aanzien van tappen zijn namelijk niet gewijzigd. Uitsluitend de wijze van technische aanlevering van de tap en de wijze waarop in de statistieken vervolgens kan worden geteld, zijn gewijzigd. Een tap op een mobiele telefoon omvat zowel spraak als data en dit was, zoals in het antwoord op vraag 1 en 2 aangegeven, vóór de nieuwe interceptiestandaard ook al het geval. Voordat deze telecommunicatie wordt opgenomen, wordt conform artikel 126m van het Wetboek van Strafvordering getoetst of aan de daarin genoemde wettelijke eisen is voldaan en of de inzet van de tap voldoet aan de proportionaliteits- en subsidiariteitsvereisten. Deze toets wordt tweemaal gedaan, te weten door de officier van justitie die de rechter-commissaris vraagt om een machtiging tot tappen en door de rechter-commissaris die de machtiging afgeeft.

Vraag 6
Deelt u de mening dat de nieuwe interceptiestandaard minder transparant is? Zo nee, waarom niet?

Antwoord 6
Nee, de nieuwe interceptiestandaard is niet minder transparant. Een tap op een mobiele telefoon omvat zowel spraak als data, dus het is feitelijk onjuist om deze taps separaat te tellen. De nieuwe standaard geeft om die reden een accurater beeld.

Vraag 7
Deelt u de mening dat met de nieuwe interceptiestandaard de kans groter is dat extreem privacygevoelige data van onschuldige mensen worden verzameld? Zo nee, waarom niet?

Antwoord 7
Nee, omdat het juridisch kader en de opsporingspraktijk ten aanzien van tappen niet zijn gewijzigd. Zoals in het antwoord op vraag 3 en 4 aan de orde is gekomen, wordt iedere tapaanvraag getoetst door de officier van justitie en de rechter-commissaris. Dit juridisch kader biedt voldoende waarborgen.

Vraag 8
Onder welke voorwaarden wordt het op dit moment rechtmatig geacht om telefoons te tappen? Welke voorwaarden gelden er als het gaat om internettaps?

Antwoord 8
De voorwaarden voor het plaatsen van een tap op alle communicatie op een mobiele telefoon, dus zowel spraak als data, zijn neergelegd in (onder andere) artikel 126m/126t van het Wetboek van Strafvordering. Er moet sprake zijn van een verdenking van een misdrijf, waarvoor een bevel tot voorlopige hechtenis kan worden gegeven en dat een ernstige inbreuk op de rechtsorde oplevert. Tevens moet het onderzoek de inzet van de tap dringend vorderen.

Vraag 9 en 10
Hoe wordt omgegaan met de zogenaamde bijvangst en met de gegevens van onschuldige mensen?
Hoe lang worden de verzamelde gegevens bewaard en wat is daar de reden van?

Antwoord 9 en 10
Conform het Wetboek van Strafvordering (art. 126cc en 126dd Sv) wordt de opgenomen communicatie bewaard tot het einde van de betreffende strafrechtelijke onderzoeken. Alle opgenomen communicatie wordt bewaard omdat dit van waarde kan zijn voor het strafrechtelijk onderzoek, zowel in belastende zin als in ontlastende zin.

Vraag 11
Hoe verhoudt de nieuwe interceptiestandaard zich tot de uitspraak van het Europese Hof over de bewaarplicht?[2]

Antwoord 11
De nieuwe interceptiestandaard heeft niets met de uitspraak van het Europees Hof over de bewaarplicht te maken. Die uitspraak betreft de bewaarplicht van zogenaamde historische (verkeers)gegevens. Dit zijn gegevens over onder meer het nummer van de oproeper en opgeroepene, tijd en duur van het gesprek en de locatie bij het begin van de verbinding. De inhoud van een gesprek valt daarmee niet onder die uitspraak.
De nieuwe interceptiestandaard heeft enkel betrekking op het opnemen van communicatie en niet op deze historische (verkeers)gegevens.

Vraag 12
Hoeveel mensen zijn er sinds begin 2014, conform de nieuwe interceptiestandaard, getapt? Hoe lang is er gemiddeld getapt? Indien deze cijfers niet worden gegeven, kunt u dan toelichten waarom niet?

Antwoord 12
Het wettelijk kader vereist dat per telefoonnummer een vordering tot het plaatsen van een tap wordt gedaan. In de statistieken kan daarom alleen het aantal taps worden weergegeven en niet het aantal personen dat getapt is. Het aantal taps zegt bovendien niet zoveel over het aantal mensen dat wordt afgeluisterd omdat verdachten doorgaans meer dan één telefoon hebben – soms wel enkele tientallen- waarmee zij communiceren. De gemiddelde duur van een tap wordt niet bijgehouden. Wel worden er cijfers verstrekt in het jaarverslag van het Ministerie van Veiligheid en Justitie over het gemiddeld aantal taps per dag. In 2014 liepen gemiddeld 1.386 taps per dag.

Vraag 13
Kan over 2014 en een deel van 2015 alsnog onderscheid worden gemaakt tussen het aantal telefoontaps en internettaps? Zo nee, waarom niet?

Antwoord 13
Nee, zoals bij de tabel in het jaarverslag van het Ministerie van Veiligheid en Justitie staat toegelicht wordt sinds de invoering van de nieuwe interceptiestandaard, zowel technisch als procedureel, geen onderscheid meer gemaakt tussen een telefoontap en een internettap. Het onderscheid in de tellingen is hiermee ook komen te vervallen.

Vraag 5 en 14
Klopt het dat de proportionaliteitsafweging in Nederland structureel anders ligt dan in veel andere landen?[3] Kunt u uw antwoord uitgebreid toelichten? Hoe vaak tapt Nederland telefoons en internet in verhouding tot andere landen, zoals bijvoorbeeld de Verenigde Staten?

---

[2] http://www.scribd.com/doc/216980523/Judgment-of-the-ECJ-in-Digital-Rights-Ireland-data-retention-challenge
[3] http://webwereld.nl/beveiliging/37737-nederland--kampioen--eigen-burgers-aftappen

Antwoord 5 en 14
Het is moeilijk een vergelijking te maken met andere landen omdat de rechtsstelsels van die landen veelal verschillend zijn. Ieder stelsel kent zijn eigen voorwaarden en waarborgen ten aanzien van de inzet van bijzondere opsporingsmiddelen zoals het opnemen van telecommunicatie. Onderzoek van het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) uit 2012 laat zien dat in Nederland een zorgvuldige afweging wordt gemaakt tussen het nut en de noodzaak van de inzet van een telefoon- en internettap in een opsporingsonderzoek.
Ook de tapstatistieken in verschillende landen laten een grote verscheidenheid zien. Dit soort cijfers zeggen overigens niets over de mate waarin de privacy in opsporingsonderzoeken wordt aangetast. Zo is bekend dat de autoriteiten in de VS andere opsporingsmethoden, zoals het plaatsen van bakens of de inzet van (criminele) infiltranten, vaker inzetten dan in Nederland. Ook wordt er niet in alle landen eenduidig geteld. In Nederland wordt bijvoorbeeld het aantal getapte nummers geteld terwijl in andere landen, bijvoorbeeld Spanje, het aantal vorderingen wordt geteld waarbij een vordering meerdere nummers kan bevatten. Dit maakt een betrouwbare cijfermatige vergelijking onmogelijk.

Vraag 15
Heeft het College Bescherming Persoonsgegevens (CBP) zich reeds uitgelaten over de nieuwe interceptiestandaard? Zo nee, waarom niet en bent u bereid alsnog het oordeel van het CBP te vragen? Zo ja, wat was het oordeel?

Antwoord 15
Nee, daartoe bestaat geen aanleiding nu de wijziging van de interceptiestandaard louter technisch en procedureel van aard is en niet leidt tot een gewijzigde verwerking van persoonsgegevens.